REMARKS

This amendment is in response to the Office Action dated February 5, 2008 (the "Office Action"). Claims 1-2, 4-16 and 18-25 are pending in the application. Claims 1-2, 10-16, and 18-24 have been amended. Claim 25 has been added. Claims 3 and 17 have been cancelled without prejudice or disclaimer. No new matter has been added.

Claims 1-2, 4-16 and 18-25 are Allowable

The Office has rejected claims 1, 10 and 15, under 35 U.S.C. §103(a), as being unpatentable over U.S. Patent No. 6,647,400 ("Moran"), in view of U.S. Application No. 2004/0049693 ("Douglas"). Further, the Office has rejected claims 2-9, 11-14 and 16-24, under 35 U.S.C. §103(a), as being unpatentable over Moran, in view of Douglas, and further in view of U.S. Patent No. 5,919,257 ("Trostle"). Claims 3 and 17 have been cancelled without prejudice or disclaimer. Applicants respectfully traverse the remainder of the rejections.

The cited portions of Moran, Douglas, and Trostle, individually or in combination, do not disclose or suggest the specific combination of claim 1. For example, the cited portions of Moran fail to disclose or suggest that upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host, and issuing a command to an operating system of the host to <u>bring the host to a single user state</u>, as in claim 1.

In contrast to claim 1, the cited portions of Moran indicate that if there is a mismatch of signatures, and if the mismatch is not expected, the file associated with the signature is flagged as suspicious. *See* Moran, col. 32, lines 56-58. The cited portions of Moran fail to disclose or suggest that upon identifying a mismatch in compared digital signatures, issuing an instruction to record an entry in a log file located in a second remote database, said entry identifying a possible intrusion in a host, and issuing a command to an operating system of the host to <u>bring the host to a single user state</u>, as in claim 1.

Further, the cited portions of Douglas fail to disclose or suggest this feature of claim 1. Instead, the cited portions of Douglas describe a host-based intrusion detection system (HIDS) sensor that monitors system logs for evidence of malicious or suspicious application activity running in real time and monitors key system files for evidence of tampering. *See* Douglas, Abstract. Further, Douglas describes providing notice about attack events associated with network security. *See* Douglas, Title. Applicants respectfully submit that providing notice about attack events is different from issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1. Therefore, the cited portions of Douglas fail to disclose or suggest at least one feature of claim 1.

The Office asserts that Trostle discloses issuing a command to an operating system of the host to bring said host to a single user state upon identifying the mismatch in compared digital signatures. *See* Office Action, p. 8. Applicants respectfully submit that, in contrast to claim 1, the cited portions of Trostle describe a login process in which if an invalid password has been entered, a server increments an intruder detection counter, and if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, Fig. 4; Fig. 5; and col. 6, lines 30-42. Applicants respectfully submit that disabling a NIC and/or disabling a workstation are different from issuing a command to an operating system of the host to bring the host to a single user state, as in claim 1. Therefore, the cited portions of Trostle fail to disclose or suggest at least one feature of claim 1.

Therefore, the cited portions of Moran, Douglas, and Trostle, individually or in combination, fail to disclose or suggest the specific combination of claim 1. Hence, claim 1 is allowable. Claims 2 and 4-9 are allowable, at least by virtue of their dependence from an allowable claim.

The cited portions of Moran, Douglas, and Trostle, individually or in combination, do not disclose or suggest the specific combination of claim 10. For example, the cited portions of Moran fail to disclose or suggest that a mismatch identifies a possible intrusion in the host, resulting in a command being issued to an operating system of the host to bring the host to a single user state, as in claim 10.

In contrast to claim 10, the cited portions of Moran indicate that if there is a mismatch of signatures, and if the mismatch is not expected, the file associated with the signature is flagged as suspicious. See Moran, col. 32, lines 56-58. The cited portions of Moran fail to disclose or suggest that a mismatch identifies a possible intrusion in the host, resulting in a command being issued to an operating system of the host to bring the host to a single user state, as in claim 10.

Further, the cited portions of Douglas fail to disclose or suggest this feature of claim 10. Instead, the cited portions of Douglas describe a host-based intrusion detection system (HIDS) sensor that monitors system logs for evidence of malicious or suspicious application activity running in real time and monitors key system files for evidence of tampering. *See* Douglas, Abstract. Further, Douglas describes providing notice about attack events associated with network security. *See* Douglas, Title. Applicants respectfully submit that providing notice about attack events is different from issuing a command to an operating system of the host to bring the host to a single user state, as in claim 10. Therefore, the cited portions of Douglas fail to disclose or suggest at least one feature of claim 10.

The Office asserts that Trostle discloses issuing a command to an operating system of the host to bring said host to a single user state upon identifying the mismatch in compared digital signatures. *See* Office Action, p. 8. Applicants respectfully submit that, in contrast to claim 10, the cited portions of Trostle describe a login process in which if an invalid password has been entered, a server increments an intruder detection counter, and if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, Fig. 4; Fig. 5; and col. 6, lines 30-42. Applicants respectfully submit that disabling a NIC and/or disabling a workstation are different from issuing a command to an operating system of the host to bring the host to a single user state, as in claim 10. Therefore, the cited portions of Trostle fail to disclose or suggest at least one feature of claim 10.

Therefore, the cited portions of Moran, Douglas, and Trostle, individually or in combination, fail to disclose or suggest the specific combination of claim 10. Hence, claim 10 is allowable. Claims 11-14 are allowable, at least by virtue of their dependence from an allowable claim.

The cited portions of Moran, Douglas, and Trostle, individually or in combination, do not disclose or suggest the specific combination of claim 15. For example, the cited portions of Moran fail to disclose or suggest computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state upon identifying a mismatch in compared digital signatures, as in claim 15.

In contrast to claim 15, the cited portions of Moran indicate that if there is a mismatch of signatures, and if the mismatch is not expected, the file associated with the signature is flagged as suspicious. See Moran, col. 32, lines 56-58. The cited portions of Moran fail to disclose or suggest computer readable program code comprising executable instructions to issue a command to an operating system of a host to bring the host to a single user state upon identifying a mismatch in compared digital signatures, as in claim 15.

Further, the cited portions of Douglas fail to disclose or suggest this feature of claim 15. Instead, the cited portions of Douglas describe a host-based intrusion detection system (HIDS) sensor that monitors system logs for evidence of malicious or suspicious application activity running in real time and monitors key system files for evidence of tampering. *See* Douglas, Abstract. Further, Douglas describes providing notice about attack events associated with network security. *See* Douglas, Title. Applicants respectfully submit that providing notice about attack events is different from issuing a command to an operating system of a host to bring the host to a single user state upon identifying a mismatch in compared digital signatures, as in claim 15. Therefore, the cited portions of Douglas fail to disclose or suggest at least one feature of claim 15.

The Office asserts that Trostle discloses issuing a command to an operating system of said host to bring said host to a single user state upon identifying the mismatch in compared digital signatures. *See* Office Action, p. 10. Applicants respectfully submit that, in contrast to claim 15, the cited portions of Trostle describe a login process in which if an invalid password has been entered, a server increments an intruder detection counter, and if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, Fig. 4; Fig. 5; and col. 6, lines 30-42.

Applicants respectfully submit that disabling a NIC and/or disabling a workstation are different from issuing a command to an operating system of a host to bring the host to a single user state upon identifying a mismatch in compared digital signatures, as in claim 15. Therefore, the cited portions of Trostle fail to disclose or suggest at least one feature of claim 15.

Therefore, the cited portions of Moran, Douglas, and Trostle, individually or in combination, fail to disclose or suggest the specific combination of claim 15. Hence, claim 15 is allowable. Claim 16 is allowable, at least by virtue of its dependence from an allowable claim.

The cited portions of Moran, Douglas, and Trostle, individually or in combination, do not disclose or suggest the specific combination of claim 18. For example, the cited portions of Moran fail to disclose or suggest issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

In contrast to claim 18, the cited portions of Moran indicate that if there is a mismatch of signatures, and if the mismatch is not expected, the file associated with the signature is flagged as suspicious. See Moran, col. 32, lines 56-58. The cited portions of Moran fail to disclose or suggest issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18.

Further, the cited portions of Douglas fail to disclose or suggest this feature of claim 18. Instead, the cited portions of Douglas describe a host-based intrusion detection system (HIDS) sensor that monitors system logs for evidence of malicious or suspicious application activity running in real time and monitors key system files for evidence of tampering. *See* Douglas, Abstract. Further, Douglas describes providing notice about attack events associated with network security. *See* Douglas, Title. Applicants respectfully submit that providing notice about attack events is different from issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18. Therefore, the cited portions of Douglas fail to disclose or suggest at least one feature of claim 18.

The Office asserts that Trostle discloses issuing a command to an operating system of the host to bring said host to a single user state upon identifying the mismatch in compared digital signatures. *See* Office Action, p. 8. Applicants respectfully submit that, in contrast to claim 18, the cited portions of Trostle describe a login process in which if an invalid password has been entered, a server increments an intruder detection counter, and if a maximum number of unsuccessful attempts to enter a correct password has been exceeded, a Network Interface Card (NIC) may be disabled to prevent subsequent workstation/server communication, or the workstation may be completely disabled. *See* Trostle, Fig. 4; Fig. 5; and col. 6, lines 30-42. Applicants respectfully submit that disabling a NIC and/or disabling a workstation are different from issuing a command to an operating system of a host to bring the host to a single user state, as in claim 18. Therefore, the cited portions of Trostle fail to disclose or suggest at least one feature of claim 18.

Therefore, the cited portions of Moran, Douglas, and Trostle, individually or in combination, fail to disclose or suggest the specific combination of claim 18. Hence, claim 18 is allowable. Claims 19-25 are allowable, at least by virtue of their dependence from an allowable claim.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the references as applied in the Office Action. Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the cited art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicants
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)

5-2-2008
Date